Document Title	Product security Risk Table
Document number / Revision	D001020017 / 01
Date	8-Apr-22
Project	SmartMedic Phase II
Project number	SGTC-NPD-001

Product Security Risk Table approval				
Approvals	**Name**	**Title**	**Signature**	**Date**
Author	Deepak Sharma	Design Engineering R&D (Software)		
Approvers	Pragya Nidhi	Test Engineering		
	Vikram Puri	Advanced Operations (Mfg & QA)		
	Sreejith Viswam	Advance Quality Engineer		

Document Revision History:

REV#	Revision Date	Author	Description of Revision
00	30-Aug-21	Deepak Sharma	Initial Release DR1-4 Document was reviewed but not approved and archived, thus archiving
01	8-Apr-22	Deepak Sharma	Document updated as per DR5-7 requirements -Security Controls/Mitigations -Security Risk Control Measures -Implementation of Risk Control Measures -Verification of Risk Control Measures (Effectiveness)

System & Asset Identification

Medical Device / System:	SmartMedic
Scope:	SmartMedic -001-02-A-00-00-00
Date:	<08 April 2022>
Conducted by:	<Author Name / Function / Organization> Deepak Sharma / Design Engineering R&D Software <Author Name / Function / Organization>

ID #	Asset Type (Information/Physical)	Asset	Asset Description
A01	*Physical Asset*	*Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)*	*Utilizing computer resources and computing power by adversary, allows various general purpose attacks, such as incl. Ransomware deployment, Bitcoin Mining, abuse of peripheral devices such as WebCam, Microphones, etc., .*
A02	*Information asset*	*Tablet OS/network details & Tablet Application*	*Information about internals of the system (Device identification, software versions, supported protocols, etc.)*
A03	*Physical Assets*	*Smart medic (Stryker device) System Component*	*Monitors local bed status information, alerting caregivers visually, audibly or remotely if preset parameters are compromised.*
A04	*Information asset*	*Authentication/Authorisation method of all device(s)/app*	*Information related to authenication/authorisation data (password/pins/MFA/Biometrics)*
A05	*Physical Assets*	*Device Maintainence tool (Hardware/Software)*	*Device Maintainence tool (Hardware/Software) that patchs and updates Smart Medic Device and Application related to Security*
A06	*Information asset*	*Electronic Health Records (EHR)/ Device Component status*	*Smart device components health status information*
A07	*Information asset*	*Interface/API Communication*	Communication middleware enables communication and data management for distributed applications.
A08	Physical Assets	Wireless Network device (Scope of HDO)	Devices that are used for communication among the Smart Medic project component.
A09	Information asset	Data at Rest	Use strong encryption algorthim to store data on cloud platform (Smartmedic Device)/tablet
A10	Information asset	Data in Transit	Use strong encryption algorthim to data moving on tablet to cloud platform(Smartmedic Device)/tablet
A11	Information asset	Smart medic app (Stryker Admin Web Application)	Smart medic application for nurse/health worker (Stryker Admin Web Application)
A12	Information asset	Smart medic app (Azure Portal Administrator)	Azure Portal Administrator for Smart medic app
A13	Information asset	Azure Cloud DataBase	Azure Cloud DataBase related to Smart Medic app
A14	Information asset	Health vital data	Health vital data Body temperature. Pulse rate. Respiration rate,weight data, position data, etc.
A15	Information asset	Nurse Station Application	Smart medic web application for nurse/health worker running on the Nurse Station

Vulnerability Identification

Vuln. ID	Vulnerability Description	Applicable (Yes/No)	Rationale (if Vulnerability not applicable)
V01	Devices with default passwords needs to be checked for bruteforce attacks	Yes	n/a
V02	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	Yes	n/a
V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	Yes	n/a
V04	Checking authentication modes for possible hacks and bypasses	Yes	n/a
V05	Insecure communications in networks (hospital)	Yes	n/a
SBOM			
V06	Lack of Asset location digaram in security operations manual	Yes	n/a
V07	Lack of configuration controls for IT assets in the informaion system plan	Yes	n/a
V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	Yes	n/a
V09	Lack of plan for periodic Software Vulnerability Management	Yes	n/a
V10	The static connection digaram between devices and applications with provision for periodic updation as per changes	Yes	n/a
V11	Assest counting system for all instances of product implementation	Yes	n/a
Access points			
V12	Unprotected network port(s) on network devices and connection points	Yes	n/a
V13	Unprotected external USB Port on the tablet/devices.	Yes	n/a
V14	Unencrypted Network segment through out the information flow	Yes	n/a
V15	Controlled Use of Administrative Privileges over the network	Yes	n/a
Data			
V16	Unencrypted data at rest in all possible locations	Yes	n/a
V17	Unencrypted data in transit in all flowchannels	Yes	n/a
V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	Yes	n/a
V19	Weak Algorthim implementation with respect cipher key size	Yes	n/a
InSecure Configurations of Resources			
V20	InSecure/not recommended Configuration for Mobile Devices, Laptops, Workstations, and Servers	Yes	n/a
V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	Yes	n/a
V22	Legacy system identification if any	Yes	n/a
V23	Outdated - Software/Hardware	Yes	n/a
V31	Improper/insufficient provisioning of IOT hub	Yes	n/a
V32	Unsecured communication with unauthenticated 3rd party devices	Yes	n/a
AuthN management			
V24	Error Info containing sensitive data for Failed Authentication attempts	Yes	n/a
V25	Absence of additional security factor along with user identification	Yes	n/a
V26	Having no limit on the login attempts	Yes	n/a
V27	No session expiry after certain time interval	Yes	n/a
Logging/Monitoring			
V28	Insufficient Logging information	Yes	n/a
V29	Insufficient Access permissions for accessing and modifying Log files	Yes	n/a
Keys & Certificates			
V30	Improper security (for ex.,Storage & Access) for Key tokens and Certificates	Yes	n/a

Printed copies for reference only

Threat Assessment

#	Threat Event	Description	Threat Source	In Scope (Yes/No)	Rationale (if out of scope)
T01	Deliver undirected malware (CAPEC-185)	Thread source delivers malware by providing removable media prepared with malware. Removable media is e.g. left on a parking lot and picked up by hospital staff. USB stick finds its way to the Navigation System. Malware eploits known a known vulnerability and e.g. gains admin priviledges. Undirected attack on computer systems.	TSA-3 - Skript Kiddies	Yes	n/a
T02	Deliver directed malware (CAPEC-185)	Thread source delivers malware on a removable media which was designed to exploit a known vulnerability of the Navigation System. Directed attack on the Navigation System using knowledge about the Navigation System.	TSA-2 Organization	Yes	n/a
T03	Gaining Access ([S]TRID[E])	This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data	TSA-2 Organization	Yes	n/a
T04	Maintaining Access (TTP)	The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.	TSA-2 Organization	Yes	n/a
T05	Clearing Track (TTP)	This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created	TSA-2 Organization	Yes	n/a
T06	Elevation of privilege (STRID[E])	Identify weaknesses of segregation in terms of administrative and user-level privileges	TSA-2 Organization	Yes	n/a
T07	Denial of service (STRI(D)E)	Find ways to exhaust or drown out legitimate requests	TSA-3 - Skript Kiddies	Yes	n/a
T08	Information disclosure (STR(I)DE)	Fuzz application parameters or arguments to impact application error disclosures. Identify open ports with their respective services. Incite confidentiality and integrity in the browser interface. Identify clear text communications. Review usage of HTTP headers and user-agent profile. Pinpoint usages of API endpoints and application backend technologies.	TSA-2 Organization	Yes	n/a
T09	Data Access (STR[I]DE)	Access user and application data e.g. by a malicious application or script	TSA-3 - Skript Kiddies	Yes	n/a
T10	Open network port exploit (TTP)	Penetrate Open and Unsecured Ports	TSA-3 - Skript Kiddies	Yes	n/a
T11	Brute-force Attack (CAPEC-112)	The brute-force attack contained a dictionary of well-known directories and authentication paradigms present in common webservers.	TSA-2 Organization	Yes	n/a
T12	Social Engineering (TTP)	create custom phishing scams, phone-based attacks and ev	TSA-3 - Skript Kiddies	Yes	n/a
T13	Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	All the actions/events should be properly logged and the content needs to be protected by proper access rights.	TSA-2 Organization	Yes	n/a
T14	Unauthorized Alterations (S[T]RIDE)	This involves modifying registry values, deleting/encrypting Confidential info and uninstalling Any secure applications and renaming/deleting all files/folders	TSA-2 Organization	Yes	n/a

Security Risk Assessment

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact: Asset	Adverse Impact: Impact Description	Adverse Impact: Safety Impact (Risk ID# or N/A)	Pre-Implementation of Security Controls: Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Controls/Mitigations: Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Post-Implementation of Security Controls: Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
1	T01	Deliver undirected malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	3.9	Low	0.20	3.5	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
2	T01	Deliver undirected malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	3.9	Low	0.2	3.5	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		
3	T01	Deliver undirected malware (CAPEC-185)	V02	External communications and exposure for communication channels from and to application and devices like tablet and smartmedic device.	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Network	Low	Low	Required	Unchanged	2.1	0.5	3.4	5.5	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		
4	T01	Deliver undirected malware (CAPEC-185)	V02	External communications and exposure for communication channels from and to application and devices like tablet and smartmedic device.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Network	Low	Low	Required	Unchanged	2.1	0.5	3.4	5.5	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
5	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		
6	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
7	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028								#N/A	#N/A		
8	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
9	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		
10	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028								#N/A	#N/A		
11	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
12	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		
13	T01	Deliver undirected malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Low	0.2	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
14	T01	Deliver undirected malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Low	0.2	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		
15	T01	Deliver undirected malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004								#N/A	#N/A		
16	T01	Deliver undirected malware (CAPEC-185)	V17	Unencrypted data in transit in all flowchannels	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Low	0.2	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA								#N/A	#N/A		

ID #	Threat Event(s)	Vulnerabilities	Adverse Impact			Pre-Implementation of Security Controls															Security Controls/Mitigations			Post-Implementation of Security Controls												
			Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
17	Deliver undirected malware (CAPEC-185) T01	Unencrypted data in transit in all flowchannels V17	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Low	0.2	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
18	Deliver undirected malware (CAPEC-185) T01	Outdated - Software/Hardware V23	Device Maintainence tool (Hardware/Software) A05	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Moderate	0.5	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028									#N/A	#N/A		
19	Deliver undirected malware (CAPEC-185) T01	Outdated - Software/Hardware V23	Smart medic (Stryker device) System Component A03	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Moderate	0.5	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA									#N/A	#N/A		
20	Deliver undirected malware (CAPEC-185) T01	Outdated - Software/Hardware V23	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
21	Deliver directed malware (CAPEC-185) T02	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers V21	Device Maintainence tool (Hardware/Software) A05	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Local	Low	High	Required	Unchanged	0.6	0.6	3.6	4.2	Moderate	0.50	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028									#N/A	#N/A		Justification
22	Deliver directed malware (CAPEC-185) T02	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers V21	Smart medic (Stryker device) System Component A03	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Local	Low	High	Required	Unchanged	0.6	0.6	3.6	4.2	Moderate	0.5	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA									#N/A	#N/A		
23	Deliver directed malware (CAPEC-185) T02	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers V21	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	Required	Unchanged	1.3	0.5	3.4	4.8	Low	0.2	3.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
24	Deliver directed malware (CAPEC-185) T02	Unprotected external USB Port on the tablet/devices. V13	Wireless Network device (Scope of HDO) A08	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	3.9	Moderate	0.5	3.7	LOW	SOM responsibility 1. Statefull Firewall 2. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present.	1. SOM D001020115 - 23. Malware Detection/Protection 2. SOM D001020115 - 05. Access control policy and management	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 1) DSTC001: GSL-STC-017									#N/A	#N/A		
25	Deliver directed malware (CAPEC-185) T02	Unprotected external USB Port on the tablet/devices. V13	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	3.9	Moderate	0.5	3.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
26	Deliver directed malware (CAPEC-185) T02	Unprotected external USB Port on the tablet/devices. V13	Smart medic app (Stryker Admin Web Application) A11	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	3.9	Low	0.2	3.5	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. Using web app the admin can able to view the functionality of different components existing in the SM platform. Admin app doesnt control any of the system components. Hence the risk associated to the SM platform with admin web app can be ignored. 3.SRS D001020097 – 2.23.2The Application shall provide facility of audit logs for storing the user activity details. 4.SRS D001020097 –2.17.5The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-029 3) DSTC001: GSL-STC-019 4) DSTC001: GSL-STC-004									#N/A	#N/A		
27	Deliver directed malware (CAPEC-185) T02	External communications and exposure for communication channels from and to application and devices like tablet and smartmedic device. V02	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	Required	Unchanged	0.9	0.6	3.6	4.5	Moderate	0.5	4.1	MEDIUM	1. Only stryker made/authenticated devices should communicate with smart medic device & tablet 2. Asset should be behind stateful firewall 3. Use secure tunnel communications channel	1. SRS D001020024 - 2.17.8 - Only Stryker made/ authenticated devices should be able to communicate with SM device and tablet. 2. SOM D001020115 - 23. Malware Detection/Protection 3. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-010 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-004									#N/A	#N/A		
28	Deliver directed malware (CAPEC-185) T02	Ineffective patch management of firware, OS and applications thoughout the information system plan V08	Device Maintainence tool (Hardware/Software) A05	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028									#N/A	#N/A		
29	Deliver directed malware (CAPEC-185) T02	Ineffective patch management of firware, OS and applications thoughout the information system plan V08	Smart medic (Stryker device) System Component A03	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2,3,4. SRS D001020025	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 NA									#N/A	#N/A		
30	Deliver directed malware (CAPEC-185) T02	Ineffective patch management of firware, OS and applications thoughout the information system plan V08	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
31	Deliver directed malware (CAPEC-185) T02	Unprotected network port(s) on network devices and connection points V12	Smart medic (Stryker device) System Component A03	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Moderate	0.5	4.3	MEDIUM	1. Only Stryker/HDO authenticated devices should communicate with smart medic device & tablet 2. Asset should be behind stateful firewall 3. Use secure tunnel communications channel	1. SRS D001020025 2. SOM D001020115 - 23. Malware Detection/Protection 3. SRS D001020025	Penetration Testing Protocol Document #: D001020037: NA 2) DSTC001: GSL-STC-001 NA									#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact			Pre-Implementation of Security Controls															Security Controls/Mitigations			Post-Implementation of Security Controls												
					Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
32	T02	Deliver directed malware (CAPEC-185)	V12 Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Network	Low	High	None	Unchanged	1.2	0.6	3.6	4.9	Low	0.2	3.9	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
33	T02	Deliver directed malware (CAPEC-185)	V21 InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A11	Smart medic app (Stryker Admin Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	None	None	High	Local	High	High	Required	Unchanged	0.3	0.6	3.6	4.0	Moderate	0.5	3.8	LOW	1. Deployed (V&V) secure system configuration model needs to be mentioned in the installation manual. 2. Establish internal and external information sources for threat intelligence and vulnerability data, monitoring them regularly and taking appropriate action for high-priority items 3. Use upgraded software, firmware 4. Never create/use credentials with personal details such as date of birth, spouse, or child's or pet's name 5. Stateful Firewall	1. Using web app the admin can able to view the functionality of different components existing in the SM platform. Admin app doesnt control any of the system components. Hence the risk associated to the SM platform with admin web app can be ignored. 2. SOM D001020115 - 23. Malware Detection/Protection 3.SRS D001020097 - 2.1.7.2 The application shall allow to upgrade the tablet application. 4. SRS D001020097 - 2.1.2.4 - Never create/use credentials with personal details such as date of birth, spouse, or child's or pet's name 5.SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-022 4) DSTC001: GSL-STC-023 5) DSTC001: GSL-STC-001									#N/A	#N/A		
34	T02	Deliver directed malware (CAPEC-185)	V21 InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	Required	Unchanged	1.3	0.5	3.4	4.8	Low	0.2	3.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
35	T02	Deliver directed malware (CAPEC-185)	V16 Unencrypted data at rest in all possible locations	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.20	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
36	T02	Deliver directed malware (CAPEC-185)	V16 Unencrypted data at rest in all possible locations	A02	Tablet OS/network details & Tablet Application	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
37	T02	Deliver directed malware (CAPEC-185)	V16 Unencrypted data at rest in all possible locations	A11	Smart medic app (Stryker Admin Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Identification of the sensitive data in storage and encryption of storage subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Use strong encryption algorithm	1. SAD /SDD-D001020099-6.7 Security 2. SOM D001020115 - 23. Malware Detection/Protection 3. SAD /SDD-D001020099-6.7 Security 4. SOM D001020115 - 05 Access control policy and management 5. SAD /SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-006 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-017 5) DSTC001: GSL-STC-006									#N/A	#N/A		
38	T03	Gaining Access ([S]TRID[E])	V12 Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	None	None	Low	Network	Low	Low	None	Unchanged	2.8	0.2	1.4	4.3	Low	0.2	2.0	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
39	T03	Gaining Access ([S]TRID[E])	V12 Unprotected network port(s) on network devices and connection points	A11	Smart medic app (Stryker Admin Web Application)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	None	Low	High	Network	Low	High	None	Unchanged	1.2	0.7	4.2	5.5	Low	0.2	4.5	MEDIUM	1. Admin application can be accessed by login credentials & MFA. Hence, strong password policies & management are required 2. Data transfer between the admin application and the smart medic components needs to be encrypted & secured. 3. Any vulnerable network ports and connection points should be identified and hardened. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Stateful firewall	1. Have to be closed before DR-8 2. SAD/SDD-D001020099-6.7 Security 3. SRS D001020097 -2.17.4 The Application shall establish technical controls to mitigate the potential for compromise to the integrity and confidentiality of health data stored on the product or removable media Since admin application shall be hosted as an independent azure web app and it shall have no open ports until there is explicit requirement. 4. SRS D001020097 - 2.25.1 -Application shall have the User Management Screen to configure and manage the users as per the roles. 5. SOM D001020115 - 23. Malware Detection/Protection	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-033 2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-007 4) DSTC001: GSL-STC-008 5) DSTC001: GSL-STC-001									#N/A	#N/A		
40	T03	Gaining Access ([S]TRID[E])	V12 Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	None	Low	None	Network	Low	Low	None	Unchanged	2.8	0.2	1.4	4.3	Low	0.20	2.0	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
41	T03	Gaining Access ([S]TRID[E])	V01 Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	Low	None	High	Physical	Low	Low	None	Unchanged	0.7	0.7	4.2	4.9	Moderate	0.50	4.6	MEDIUM	1.During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Maintain Access Logs	1. Have to be closed before DR-8 2.SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4.SRS D001020097 – 2.23.2 The Application shall provide facility of audit logs for storing the user activity details.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-019									#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities	Adverse Impact			Pre-Implementation of Security Controls																Security Controls/Mitigations			Post-Implementation of Security Controls												
				Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
42	T03	V01	Devices with default passwords needs to be checked for bruteforce attacks	A07	Interface/API Communication	NA	Low	None	Low	Physical	Low	Low	None	Unchanged	0.7	0.4	2.5	3.2	Low	0.2	2.7	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	1. Have to be closed before DR-8 2. SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs 6.SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-006									#N/A	#N/A		
43	T03	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04	Authentication/Authorisation method of all device(s)/app	NA	Low	None	High	Local	Low	Low	Required	Unchanged	1.3	0.7	4.2	5.6	Low	0.2	4.5	MEDIUM	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3 Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	1.Have to be closed before DR-8 2. SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs 6. SAD/SDD-D001020099-6.7 Security	1) DSTC001: GSL-STC-033 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031 8) DSTC001: GSL-STC-006									#N/A	#N/A		
44	T03	V04	Checking authentication modes for possible hacks and bypasses	A04	Authentication/Authorisation method of all device(s)/app	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error mesnages upon validation of credentials to mitigate risk of account harvesting or enumeration	1. SRS D001020097 – 2.1.2.3The Application shall have the 'Remember me' feature for login credentials and all the data which we shall store inside local storage shall be encrypted. SAD/SDD-D001020099-6.7 Security 2.SAD/SDD-D001020099-6.7 Security SRS D001020023-2.1.1.2System shall store patient id in anonymized fashion. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4.SRS D001020097 –2.1.7.1.1 Something went wrong with API operation try again / contact API admin. SRS D001020023-2.1.4.1.1 Something went wrong with API operation try again / contact API admin.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-012 2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-013 5) DSTC001: GSL-STC-009 6) DSTC001: GSL-STC-014 7) DSTC001: GSL-STC-015 8)DSTC001: GSL-STC-015									#N/A	#N/A		
45	T03	V04	Checking authentication modes for possible hacks and bypasses	A11	Smart medic app (Stryker Admin Web Application)	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration	1. SRS D001020097 – 2.1.2.3The Application shall have the 'Remember me' feature for login credentials and all the data which we shall store inside local storage shall be encrypted. SAD/SDD-D001020099-6.7 Security 2.SAD/SDD-D001020099-6.7 Security 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. 4.SRS D001020097 –2.1.7.1.1 Something went wrong with API operation try again / contact API admin.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-012 2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-015									#N/A	#N/A		
46	T03	V04	Checking authentication modes for possible hacks and bypasses	A12	Smart medic app (Azure Portal Administrator)	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
47	T03	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Ressources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	NA	Low	Low	Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	3.4	3.9	Low	0.2	3.5	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3. SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003									#N/A	#N/A		
48	T04	V02	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	NA	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Moderate	0.5	3.8	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	1. Have to be closed before DR-8 2.SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3.SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs 6.SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031 8) DSTC001: GSL-STC-006									#N/A	#N/A		
49	T04	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04	Authentication/Authorisation method of all device(s)/app	NA	Low	Low	Low	Local	Low	Low	Required	Unchanged	1.3	0.5	3.4	4.8	Low	0.2	3.7	LOW	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	1. Have to be closed before DR-8 2. SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs 6. SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-033 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031 8) DSTC001: GSL-STC-006									#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact: Asset	Adverse Impact: Impact Description	Adverse Impact: Safety Impact (Risk ID# or N/A)	Pre-Implementation of Security Controls: Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Controls/Mitigations: Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Post-Implementation of Security Controls: Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
50	T05	Clearing Track (TTP)	V21 InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	NA	Low	Low	Low	Local	Low	Low	Required	Unchanged	1.3	0.5	3.4	4.8	Low	0.2	3.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
51	T05	Clearing Track (TTP)	V23 Outdated - Software /Hardware	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Physical	Low	Low	None	Unchanged	0.7	0.5	3.4	4.1	Moderate	0.5	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
52	T05	Clearing Track (TTP)	V07 Lack of configuration controls for IT assets in the informaion system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Local	Low	Low	Required	Unchanged	1.3	0.5	3.4	4.8	Low	0.2	3.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
53	T05	Clearing Track (TTP)	V07 Lack of configuration controls for IT assets in the informaion system plan	A05	Device Maintainence tool (Hardware /Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Local	Low	Low	Required	Unchanged	1.3	0.5	3.4	4.8	Low	0.2	3.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028									#N/A	#N/A		
54	T05	Clearing Track (TTP)	V08 Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	None	Low	Low	Local	Low	High	None	Unchanged	0.8	0.4	2.5	3.4	Moderate	0.5	3.0	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
55	T05	Clearing Track (TTP)	V08 Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware /Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-028									#N/A	#N/A		
56	T05	Clearing Track (TTP)	V08 Ineffective patch management of firware, OS and applications thoughout the information system plan	A02	Tablet OS/network details & Tablet Application	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
57	T05	Clearing Track (TTP)	V10 The static connection digaram between devices and applications with provision for periodic updation as per changes	A05	Device Maintainence tool (Hardware /Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Device maintainence tool not implemented/existing in the SM platform.	1) DSTC001: GSL-STC-028									#N/A	#N/A		
58	T05	Clearing Track (TTP)	V10 The static connection digaram between devices and applications with provision for periodic updation as per changes	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and Risk Matrix SmartMedic Document # D001020010)	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
59	T06	Elevation of privilege (STRID(E))	V15 Controlled Use of Administrative Privileges over the network	A04	Authentication/Authorisation method of all device(s)/app	1) Gaining access to the portal 2) Accessing confidential data, 3) Lead misuse of confidential data 4) Company defamation	NA	Low	Low	Low	Network	Low	Low	Required	Unchanged	2.1	0.5	3.4	5.5	Low	0.2	3.8	LOW	1. Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. 2. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. 3. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).	1.SRS D001020023 -2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login 2. SAD D001020032 5.3 TCP/IP Communication 3. Have to be closed before DR-I	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-024 2) DSTC001: GSL-STC-025 3) DSTC001: GSL-STC-026 4) DSTC001: GSL-STC-029									#N/A	#N/A		
60	T06	Elevation of privilege (STRID(E))	V15 Controlled Use of Administrative Privileges over the network	A12	Smart medic app (Azure Portal Administrator)	1) Gaining access to the portal 2) Accessing confidential data, 3) Lead misuse of confidential data 4) Company defamation	NA	None	Low	High	Network	Low	High	Required	Unchanged	0.9	0.7	4.2	5.2	Moderate	0.5	4.7	MEDIUM	1. Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. 2. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. 3. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
61	T07	Denial of service (STRI(D)E)	V12 Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Bring down the service availability 2) Blocking the end user usage	NA	None	None	High	Network	Low	Low	None	Unchanged	2.8	0.6	3.6	6.5	Low	0.2	4.2	MEDIUM	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
62	T08	Information disclosure (STR(I)DE)	V16 Unencrypted data at rest in all possible locations	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	Low	Low	Local	High	High	None	Unchanged	0.5	0.5	3.4	3.9	Moderate	0.5	3.7	LOW	1. Identification of the sensitive data in storage and encryption of storage subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Use strong encrption algorithm	1. SRS D001020097 - 2.1.2.3The Application shall have the 'Remember me' feature for login credentials and all the data which we shall store inside local storage shall be encrypted. 2. SOM D001020115 - 23. Malware Detection/Protection 3. SAD/SDD-D001020099-6.7 Security 4. SRS D001020097 - 2.25.1 /Application shall have the User Management Screen to configure and manage the users as per the roles. 5.SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-012 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-008 5) DSTC001: GSL-STC-006									#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact			Pre-Implementation of Security Controls															Security Controls/Mitigations			Post-Implementation of Security Controls											
					Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
63	T08	Information disclosure (STRI)(IDE)	V17	Unencrypted data in transit in all flowchannels	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	None	Low	Network	High	Low	None	Unchanged	1.6	0.4	2.5	4.2	Moderate	0.5	3.4	LOW	1. Use secure tunnel communication channel 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. For sensitive data proper encryption mechanism needs to be designed & implemented	1. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel SRS D001020023 -2.13.3The Application shall provide secure tunnel Communications channel 2. SOM D001020115 - 16. Transmission confidentiality and integrity 3. SOM D001020115 - 23. Malware Detection/Protection 4. SOM D001020115 - 05. Access control policy and management 5. SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-004 2) DSTC001: GSL-STC-004 3) DSTC001: GSL-STC-016 4) DSTC001: GSL-STC-001 5) DSTC001: GSL-STC-017 6) DSTC001: GSL-STC-006									#N/A	#N/A		
64	T08	Information disclosure (STRI)(IDE)	V18	Weak Encryption Implementation in data at rest and in transit tactical and design wise	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	Low	Low	Local	High	High	None	Unchanged	0.5	0.5	3.4	3.9	Moderate	0.5	3.7	LOW	1. Implement server-side encryption using Service-Managed keys/recomended practise by azure. 2. Proper way of network access control 3. Encryption for sensitive data in transit, for ex: when files are moved to cloud storage, etc.. 4. Transfer over encrypted tunnel 5. Use strong encryption algorithm	1. NSA-SDD-D001020110-4.2.2-Azure Cloud Infrastructure 2. SOM D001020115 - 05. Access control policy and management 3. SAD/SDD-D001020099-6.7 Security Tablet-SDD-D001020040-6.7-Security NSA-SAD-D001020031-6.7-Security 4. SRS D001020024 – 2.17.2The Application shall provide secure tunnel Communications channel SRS D001020023- 2.13.3The Application shall provide secure tunnel Communications channel NSA-SDD-D001020110-4.2.1-Nurse Station Web Services 5. NSA-SAD-D001020031-6.7-Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-020 2) DSTC001: GSL-STC-017 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-006 5) DSTC001: GSL-STC-006 6) DSTC001: GSL-STC-004 7) DSTC001: GSL-STC-004 8) DSTC001: GSL-STC-021 9) DSTC001: GSL-STC-006									#N/A	#N/A		
65	T08	Information disclosure (STRI)(IDE)	V18	Weak Encryption Implementation in data at rest and in transit tactical and design wise	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	None	Low	Network	High	Low	None	Unchanged	1.6	0.4	2.5	4.2	Moderate	0.5	3.4	LOW	1. Statefull firewall 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Use secure tunnel communication channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SOM D001020115 - 16. Transmission confidentiality and integrity 3. SOM D001020115 - 23. Malware Detection/Protection 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-016 3) DSTC001: GSL-STC-001 4) DSTC001: GSL-STC-004									#N/A	#N/A		
66	T08	Information disclosure (STRI)(IDE)	V19	Weak Algorithm implementation with respect cipher key size	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	Low	Low	Local	High	High	None	Unchanged	0.5	0.5	3.4	3.9	Moderate	0.5	3.7	LOW	1. Weak algorithms such as DES, RC4, etc.. should be avoided and usage of strong algorithms such as AES, RSA, etc.. are recomended 2. Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.	1. SRS D001020097 –2.8.1Application shall use APIs to communicate between browser application and the backend. 2. SRS D001020097 –2.8.1Application shall use APIs to communicate between browser application and the backend.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-011 2) DSTC001: GSL-STC-011									#N/A	#N/A		
67	T08	Information disclosure (STRI)(IDE)	V19	Weak Algorithm implementation with respect cipher key size	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	None	Low	Network	High	Low	None	Unchanged	1.6	0.4	2.5	4.2	Moderate	0.5	3.4	LOW	1. Weak algorithms such as DES, RC4, etc.. should be avoided and usage of strong algorithms such as AES, RSA, etc.. are recomended 2. Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.	1. SRS D001020097 –2.8.1Application shall use APIs to communicate between browser application and the backend. 2. SRS D001020097 –2.8.1Application shall use APIs to communicate between browser application and the backend.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-011 2) DSTC001: GSL-STC-011									#N/A	#N/A		
68	T08	Information disclosure (STRI)(IDE)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	Low	Low	Network	High	High	None	Unchanged	0.7	0.5	3.4	4.1	Moderate	0.5	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
69	T08	Information disclosure (STRI)(IDE)	V14	Unencrypted Network segment through out the information flow	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	None	Low	Network	High	Low	None	Unchanged	1.6	0.4	2.5	4.2	Moderate	0.5	3.4	LOW	1. Anonymization/Pseudomyzation of patient details 2. Data encyprtion 3. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 4. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.)	1.SRS D001020023- 2.1.6.21The Application shall allow to assign and edit patient reference ID to patient. 2. SAD/SDD-D001020099-6.7 Security Tablet-SDD-D001020040-6.7-Security NSA-SAD-D001020031-6.7-Security 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices.).	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-005 2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-006 5) DSTC001: GSL-STC-003 6) DSTC001: GSL-STC-003									#N/A	#N/A		
70	T08	Information disclosure (STRI)(IDE)	V05	Insecure communications in networks (hospital)	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	Low	None	Low	Network	High	Low	None	Unchanged	1.6	0.4	2.5	4.2	Moderate	0.5	3.4	LOW	1. Secure communication with Secure Sockets Layer (SSL) or TLS protocols that provide message confidentiality 2. Secure sensitive data in the channel flow using strong encryption 3. Statefull firewall 4. Proper way of network access control	1. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel 2. SAD/SDD-D001020099-6.7 Security 3. SOM D001020115 - 23. Malware Detection/Protection 4. SOM D001020115 - 05. Access control policy and management	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-004 2) DSTC001: GSL-STC-006 3) DSTC001: GSL-STC-001 4) DSTC001: GSL-STC-017									#N/A	#N/A		
71	T09	Data Access (STRI)(IDE)	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	None	None	High	Network	High	High	None	Unchanged	0.7	0.6	3.6	4.4	Low	0.2	3.8	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		
72	T09	Data Access (STRI)(IDE)	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	None	Low	Low	Network	High	High	None	Unchanged	0.7	0.4	2.5	3.3	Low	0.2	2.7	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004									#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact			Pre-Implementation of Security Controls														Security Controls/Mitigations			Post-Implementation of Security Controls												
					Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
73	T09	Data Access (STRIJDE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A09	Data at Rest	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	Low	Low	Low	Network	High	High	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Statefull firewall 3. Do not store sensitive data in plaintext. 4. Use strong encrption algorithm. 5. Apply salting over sensitive data.	1. Have to be closed before DR-8 2. SOM D001020115 - 23. Malware Detection/Protection 3. SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized fashion. 4.SAD/SDD-D001020099-6.7 Security 5.SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized fashion.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-013 5) DSTC001: GSL-STC-006 6) DSTC001: GSL-STC-006 7) DSTC001: GSL-STC-013										#N/A	#N/A		
74	T09	Data Access (STRIJDE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	High	None	None	Network	High	High	None	Unchanged	0.7	0.6	3.6	4.4	Moderate	0.5	4.0	MEDIUM	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Statefull firewall 3. Do not store sensitive data in plaintext. 4. Use strong encrption algorithm. 5. Apply salting over sensitive data.	1. Have to be closed before DR-8 2. SOM D001020115 - 23. Malware Detection/Protection 3. SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized fashion. 4.SAD/SDD-D001020099-6.7 Security 5.SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized fashion.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-013 5) DSTC001: GSL-STC-006 6) DSTC001: GSL-STC-006 7) DSTC001: GSL-STC-013										#N/A	#N/A		
75	T09	Data Access (STRIJDE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A10	Data in Transit	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	High	None	None	Network	High	High	None	Unchanged	0.7	0.6	3.6	4.4	Low	0.2	3.8	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Statefull firewall 3 Do not store sensitive data in plaintext. 4. Use strong encrption algorithm. 5. Apply salting over sensitive data.	1. Have to be closed before DR-8 2. SOM D001020115 - 23. Malware Detection/Protection 3. SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized fashion. 4.SAD/SDD-D001020099-6.7 Security 5.SAD/SDD-D001020099-6.7 Security SRS D001020023-2.13.2System shall store patient id in anonymized fashion.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-001 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-013 5) DSTC001: GSL-STC-006 6) DSTC001: GSL-STC-006 7) DSTC001: GSL-STC-013										#N/A	#N/A		
76	T09	Data Access (STRIJDE)	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A09	Data at Rest	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	Low	Low	Low	Network	High	High	None	Unchanged	0.7	0.5	3.4	4.1	Low	0.2	3.6	LOW	1. Strong password strength practices is recommended for admin web app. 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	1. Have to be closed before DR-8 2. SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs 6. SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-033 2) DSTC001: GSL-STC-02 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-009 5) DSTC001: GSL-STC-014 6) DSTC001: GSL-STC-031 7) DSTC001: GSL-STC-031 8) DSTC001: GSL-STC-006										#N/A	#N/A		
77	T09	Data Access (STRIJDE)	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	None	Low	Low	Physical	High	High	None	Unchanged	0.2	0.4	2.5	2.7	Moderate	0.5	2.6	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004										#N/A	#N/A		
78	T10	Open network port exploit (TTP)	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Capture your account's user ID and credentials. 2) Log the data of online traffic accessed on your tablet or computer. In this way, they can maintain a data of the websites you mostly visit, and plan attack from these websites. 3) Gain access to your computer, its network and data. 4) Launch a spam or malware attack on your device.	NA	None	None	Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	3.1	Moderate	0.5	2.3	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004										#N/A	#N/A		
79	T10	Open network port exploit (TTP)	V12	Unprotected network port(s) on network devices and connection points	A08	Wireless Network device (Scope of HDO)	1) Capture your account's user ID and credentials. 2) Log the data of online traffic accessed on your tablet or computer. In this way, they can maintain a data of the websites you mostly visit, and plan attack from these websites. 3) Gain access to your computer, its network and data. 4) Launch a spam or malware attack on your device.	NA	None	None	Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	3.1	Moderate	0.5	2.3	LOW	SOM responsibility 1. Statefull firewall and using port security on firwall 2. Configure router wireless security options based on manufacture manual	1. SOM D001020115 - 23. Malware Detection/Protection 2. SOM D001020115 -11. Configuration settings	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 1) DSTC001: GSL-STC-032										#N/A	#N/A		
80	T10	Open network port exploit (TTP)	V14	Unencrypted Network segment through out the information flow	A02	Tablet OS/network details & Tablet Application	1) Capture your account's user ID and credentials. 2) Log the data of online traffic accessed on your tablet or computer. In this way, they can maintain a data of the websites you mostly visit, and plan attack from these websites. 3) Gain access to your computer, its network and data. 4) Launch a spam or malware attack on your device.	NA	None	None	Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	3.1	Moderate	0.5	2.3	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004										#N/A	#N/A		
81	T10	Open network port exploit (TTP)	V17	Unencrypted data in transit in all flowchannels	A10	Data in Transit	1) Capture your account's user ID and credentials. 2) Log the data of online traffic accessed on your tablet or computer. In this way, they can maintain a data of the websites you mostly visit, and plan attack from these websites. 3) Gain access to your computer, its network and data.	NA	None	None	Low	Network	High	Low	None	Unchanged	1.6	0.2	1.4	3.1	Moderate	0.5	2.3	LOW	1. Use secure tunnel communication channel 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. For sensitive data proper encryption mechanism needs to be designed & implemented	1. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel SRS D001020023 -2.13.2The Application shall provide secure tunnel Communications channel 2. SOM D001020115 - 16. Transmission confidentiality and integrity 3. SOM D001020115 - 23. Malware Detection/Protection 4. SOM D001020115 - 05. Access control policy and management 5. SAD/SDD-D001020099-6.7 Security"	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-004 2) DSTC001: GSL-STC-004 3) DSTC001: GSL-STC-016 4) DSTC001: GSL-STC-001 5) DSTC001: GSL-STC-017 6) DSTC001: GSL-STC-006										#N/A	#N/A		
82	T10	Open network port exploit (TTP)	V05	Insecure communications in networks (hospital)	A02	Tablet OS/network details & Tablet Application	1) Capture your account's user ID and credentials. 2) Log the data of online traffic accessed on your tablet or computer. In this way, they can maintain a data of the websites you mostly visit, and plan attack from these websites. 3) Gain access to your computer, its network and data. 4) Launch a spam or malware attack on your device.	NA	None	Low	Low	Network	High	Low	None	Unchanged	1.6	0.4	2.5	4.2	Moderate	0.5	3.4	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	1. SOM D001020115 - 23. Malware Detection/Protection 2.SRS D001020024 -2.17.6The Application shall support the use of anti-malware mechanism 3.SRS D001020024 -2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices). 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-002 3) DSTC001: GSL-STC-003 4) DSTC001 - GSL-STC-004										#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact			Pre-Implementation of Security Controls														Security Controls/Mitigations			Post-Implementation of Security Controls											
					Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
83	T11	Brute-force Attack (CAPEC-112)	V01 Devices with default passwords needs to be checked for bruteforce attacks	A11	Smart medic app (Stryker Admin Web Application)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	None	Low	Network	High	High	None	Unchanged	0.7	0.4	2.5	3.3	Moderate	0.5	2.9	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.)	1. Have to be closed before DR-8 2. SRS D001020097 - 2.1.2.6 The Application shall be validated by using an invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029 2) DSTC001: GSL-STC-025 3) DSTC001: GSL-STC-009 4) DSTC001: GSL-STC-014 5) DSTC001: GSL-STC-031 6) DSTC001: GSL-STC-031									#N/A	#N/A		
84	T11	Brute-force Attack (CAPEC-112)	V01 Devices with default passwords needs to be checked for bruteforce attacks	A12	Smart medic app (Azure Portal Administrator)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	None	Low	Network	High	High	None	Unchanged	0.7	0.4	2.5	3.3	Moderate	0.5	2.9	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.)	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
85	T11	Brute-force Attack (CAPEC-112)	V03 The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A11	Smart medic app (Stryker Admin Web Application)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	None	Low	Network	High	High	None	Unchanged	0.7	0.4	2.5	3.3	Moderate	0.5	2.9	LOW	1. Strong password strength practices is recommended for admin web app. 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	1. Have to be closed before DR-8 2. SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. 3. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left. 4. SRS D001020097 - 2.23.2 - Audit logs 5. SRS D001020097 - 2.23.2 - Audit logs 6. SAD/SDD-D001020099-6.7 Security"	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-033 2) DSTC001: GSL-STC-024 3) DSTC001: GSL-STC-025 4) DSTC001: GSL-STC-031 5) DSTC001: GSL-STC-031 6) DSTC001: GSL-STC-006									#N/A	#N/A		
86	T11	Brute-force Attack (CAPEC-112)	V03 The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A12	Smart medic app (Azure Portal Administrator)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	None	Low	Network	High	High	None	Unchanged	0.7	0.4	2.5	3.3	Moderate	0.5	2.9	LOW	1. Strong password strength practices is recommended in azure 2. Require multi-factor authentication 3. limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
87	T11	Brute-force Attack (CAPEC-112)	V18 Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A09	Data at Rest	1) An attacker may attempt to discover a weak encryption by systematically trying every possible combination of decryption key.	NA	Low	None	Low	Local	High	High	None	Unchanged	0.5	0.4	2.5	3.0	Moderate	0.5	2.8	LOW	1. Implement server-side encryption using Service-Managed keys (provided for azure) 2. Proper way of network access control 3. Encryption for sensitive data in transit, for ex: when files are moved to cloud storage, etc., 4. Transfer over encrypted tunnel 5. Use strong encryption algorithm	1. NSA-SDD-D001020110-4.2.2-Azure Cloud Infrastructure 2. SOM D001020115 - 05. Access control policy and management 3. SAD/SDD-D001020099-6.7 Security Tablet-SDD-D001020040-6.7-Security NSA-SAD-D001020031-6.7-Security 4. SRS D001020024 - 2.17.2The Application shall provide secure tunnel Communications channel SRS D001020023- 2.13.3The Application shall provide secure tunnel Communications channel NSA-SDD-D001020110-4.2.1-Nurse Station Web Services 5. NSA-SAD-D001020031-6.7-Security"	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-020 2) DSTC001: GSL-STC-017 3) DSTC001: GSL-STC-006 4) DSTC001: GSL-STC-006 5) DSTC001: GSL-STC-006 6) DSTC001: GSL-STC-004 7) DSTC001: GSL-STC-004 8) DSTC001: GSL-STC-021 9) DSTC001: GSL-STC-006									#N/A	#N/A		
88	T11	Brute-force Attack (CAPEC-112)	V18 Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A10	Data in Transit	1) An attacker may attempt to discover a weak encryption by systematically trying every possible combination of decryption key.	NA	Low	None	Low	Network	High	High	None	Unchanged	0.7	0.4	2.5	3.3	Moderate	0.5	2.9	LOW	1. Statefull firewall 2. Configure and upgrade routers for the s/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Use secure tunnel communication channel	1. SOM D001020115 - 23. Malware Detection/Protection 2. SOM D001020115 - 16. Transmission confidentiality and integrity 3. SOM D001020115 - 23. Malware Detection/Protection 4. SRS D001020024 -2.17.2The Application shall provide secure tunnel Communications channel	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-001 2) DSTC001: GSL-STC-016 3) DSTC001: GSL-STC-001 4) DSTC001: GSL-STC-004									#N/A	#N/A		
89	T12	Social Engineering (TTP)	V22 Legacy system identification if any	A11	Smart medic app (Stryker Admin Web Application)	1) This threat may hamper digital or physical resources, infractructure and end points 2) Get the user (employee/ client/ customer) to download malware, send money or perform actions that are dangerous.	NA	None	Low	High	Adjacent Network	High	High	Required	Unchanged	0.4	0.7	4.2	4.6	Moderate	0.5	4.5	MEDIUM	Stryker IT team responsibility 1. Ignore/Delete any request seeking for personal info from 3rd parties 2. Statefull firewall 3. Disable device network discoverable 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present.	Using web app the admin can able to view the functionality of different components existing in the SM platform. Admin app doesnt control any of the system components. Hence the risk associated to the SM platform with admin web app can be ignored.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
90	T12	Social Engineering (TTP)	V04 Checking authentication modes for possible hacks and bypasses	A07	Interface/API Communication	1) This threat may hamper digital or physical resources, infractructure and end points through spear phishing mail 2) Get the user (employee/ client/ customer) to download malware, send money or perform actions that are dangerous. 3) Reputational harm 4) Economical harm	NA	None	Low	High	Adjacent Network	High	High	Required	Unchanged	0.4	0.7	4.2	4.6	Moderate	0.5	4.5	MEDIUM	Stryker IT team responsibility 1. Set your spam filters setting options to high 2. Restrict the system getting connected to unauthenticated sources 3. Restrict the system in accessing the 3rd party sites, social engineering sites, mails, etc., 4. Configure firewalls to reject any packets with spoofed addresses.	The setup & configuration process of azure cloud admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
91	T13	Lack of evidence to conclude any malicious attempt/attack (STRIDE)	V28 Insufficient Logging information	A12	Smart medic app (Azure Portal Administrator)	1) Adversary tried to obtain knowledge about system internals 2) Attempt to find attack vectors 3) Executed malicious activities 4) Complete details related to the attacker/malicious activities not recorded	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	Audit/System log: All the information needed for identifying the threat (malicious) activity and adversary information needed to be logged for determining the attack vector and attack surface. This helps to make the system less vulnerable in future by correcting those issues.	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
92	T13	Lack of evidence to conclude any malicious attempt/attack (STRIDE)	V29 Insufficient Access permissions for accessing and modifying Log files	A12	Smart medic app (Azure Portal Administrator)	1) Adversary tried to obtain knowledge about system internals 2) Attempt to find attack vectors 3) Executed malicious activities 4) Complete details related to the attacker/malicious activities not recorded	NA	Low	Low	Low	Local	Low	Low	None	Unchanged	1.8	0.5	3.4	5.3	Low	0.2	3.8	LOW	Audit/System log & security: 1. All the information needed for identifying the threat (malicious) activity and adversary information needed to be logged for determining the attack vector and attack surface. This helps to make the system less vulnerable in future by correcting those issues. 2. Audit/System log should be secured from unauthorized access.	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
93	T03	Gaining Accessn ([S]TRID[E])	V24 Error Info containing sensitive data for Failed Authentication attempts	A12	Smart medic app (Azure Portal Administrator)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	Low	High	Network	High	Low	None	Unchanged	1.6	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM	1. Standard error info messages should be used. Information aiding the attacks should be avoided. 2. Apart from user id there should be additional security factor for verification. 3. Limit on the login attempts is mandatory.	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		
94	T03	Gaining Accessn ([S]TRID[E])	V30 Improper security (for ex.,Storage & Access) for Key tokens and Certificates	A13	Azure Cloud DataBase	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	Low	High	Network	High	Low	None	Unchanged	1.6	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM	1. If database access using keys/certificates, their generation & storage should be done securely. 2. Apart from user id there should be additional security factor (keys/certificates) for verification. 3. Limit on the login attempts is mandatory.	1,2. SAD - D001020031 - 2.2.1.7 - Cosmos DB 3. Have to be closed before DR-8	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-027 2) DSTC001: GSL-STC-029									#N/A	#N/A		
95	T03	Gaining Accessn ([S]TRID[E])	V25 Absence of additional security factor along with user identification	A12	Smart medic app (Azure Portal Administrator)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA	Low	Low	High	Network	High	Low	None	Unchanged	1.6	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM	1. Azure portal can be accessed by login credentials & MFA. Hence, strong password policies & management are required 2. If database access using keys/certificates, their generation & storage should be done securely. 3. Apart from user id there should be additional security factor for verification. 4. Limit on the login attempts is mandatory.	The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-029									#N/A	#N/A		

ID #	Threat Event(s)		Vulnerabilities		Adverse Impact			Pre-Implementation of Security Controls															Security Controls/Mitigations			Post-Implementation of Security Controls												
					Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level	Security Risk Control Measures	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	Confidentiality	Integrity	Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Level	Residual Security Risk Acceptability Justification
96	Gaining Accrss ([S][TRID][E])	Absence of additional security factor along with user identification		Azure Cloud DataBase	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA																1. If database access provided & also using keys/certificates, their generation & storage should be done securely. 2. Apart from user id there should be additional security factor [keys/certificates] for verification. 3. Limit on the login attempts is mandatory.	1. SAD - D001020031 - 2.2.1.7 - Cosmos DB 2. SAD - D001020031 - 2.2.1.7 - Cosmos DB 3. Have to be closed before DR-II	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-027 2) DSTC001: GSL-STC-027 3) DSTC001: GSL-STC-029											
	T03	V25		A13	Low	Low	High	Network	High	Low	None	Unchanged	1.6	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM												#N/A	#N/A		
97	Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts		Azure Cloud DataBase	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA																1. Standard error info messages should be used. Information aiding the attacks should be avoided. 2. Apart from user id there should be additional security factor for verification. 3. Limit on the login attempts is mandatory.	1. SRS D001020023- 2.17.3 Generic messages should be displayed upon validation of credentials to mitigate the risk of account harvesting and enumeration. 2. SAD - D001020031 - 2.2.1.7 - Cosmos DB 3. Have to be closed before DR-II	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-018 2) DSTC001: GSL-STC-027 3) DSTC001: GSL-STC-029											
	T11	V24		A13	Low	Low	High	Network	High	Low	None	Unchanged	1.6	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM												#N/A	#N/A		
98	Brute-force Attack (CAPEC-112)	Having no limit on the login attempts		Smart medic app (Azure Portal Administrator)	1) An attacker may attempt to discover a weak credential by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.	NA																1. Standard error info messages should be used. Information aiding the attacks should be avoided. 2. Apart from user id there should be additional security factor for verification. 3. Limit on the login attempts is mandatory.	1. The setup & configuration process of azure cloud & admin shall be documented and published within the organization for the corresponding teams using the admin portal 2 - SAD - D001020031 - 2.2.1.7 - Cosmos DB 3. The setup & configuration process of azure cloud & admin shall be documented and published within the	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-018 2) DSTC001: GSL-STC-027 3) DSTC001: GSL-STC-029											
	T11	V26		A12	Low	Low	High	Network	High	Low	None	Unchanged	1.6	0.7	4.7	6.4	Moderate	0.5	5.6	MEDIUM												#N/A	#N/A		
99	Unauthorized Alterations ([T][RIDE])	Improper/insufficient provisioning of IOT hub		Tablet OS/network details & Tablet Application	1. If provisioning got failed/misleaded then the complete functionality gets affected. 2. Proper reason for the provisioning failure needs to addressed	NA																1. All devices which need to be registered & gets communicated in iot hub needs to be identified 2. Proper provisioning needs to be established with secure data transfer during provisioning 3. End-to-end provisioning with iot hub needs to be carried out without getting failed 4. All failure cases during the provisioning need to be documented/addressed	Have to be closed before DR-II	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-026											
	T14	V31		A02	None	None	High	Network	High	High	None	Unchanged	0.7	0.6	3.6	4.4	Low	0.2	3.8	LOW												#N/A	#N/A		
100	Unauthorized Alterations ([T][RIDE])	Unsecured communication with unauthenticated 3rd party devices		Tablet OS/network details & Tablet Application	If there is no proper authentication between the devices in the smart medic environment then 3rd party devices can easily establish the communication with the stryker devices	NA																1. In complete smart medic environment, only authenticated stryker and HDO devices need to be present 2. Secure communication between the stryker devices needs to be established & documented 3. Handling of the unauthenticated 3rd party devices trying to communicate with stryker devices needs to be taken care	1. Have to be closed before DR-II 2. SRS D001020024 - 2.17.8 - Only Stryker made / authenticated devices should be able to communicate with SM device and tablet. 3. SRS D001020024 - 2.17.8 - Only Stryker made / authenticated devices should be able to communicate with SM device and tablet.	Penetration Testing Protocol Document #: D001020037: 1) DSTC001: GSL-STC-030 2) DSTC001: GSL-STC-010 3) DSTC001: GSL-STC-010											
	T14	V32		A02	None	None	High	Network	High	High	None	Unchanged	0.7	0.6	3.6	4.4	Low	0.2	3.8	LOW												#N/A	#N/A		

Security Risk Assessment Summary

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
5	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
6	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
7	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
8	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
9	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
10	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
11	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
12	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
13	T01	Deliver undirected malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
14	T01	Deliver undirected malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
15	T01	Deliver undirected malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
16	T01	Deliver undirected malware (CAPEC-185)	V17	Unencrypted data in transit in all flowchannels	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
17	T01	Deliver undirected malware (CAPEC-185)	V17	Unencrypted data in transit in all flowchannels	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
18	T01	Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
19	T01	Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
20	T01	Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
21	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		Justification
22	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
23	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
24	T02	Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A08	Wireless Network device (Scope of HDO)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	SOM responsibility 1. Statefull Firewall 2. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present.		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
25	T02	Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
26	T02	Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A11	Smart medic app (Stryker Admin Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
27	T02	Deliver directed malware (CAPEC-185)	V02	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**MEDIUM**	1. Only stryker made/authenticated devices should communicate with smart medic device & tablet 2. Asset should be behind stateful firewall 3. Use secure tunnel communications channel		
28	T02	Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
29	T02	Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
30	T02	Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
31	T02	Deliver directed malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**MEDIUM**	1. Only Stryker/HDO authenticated devices should communicate with smart medic device & tablet 2. Asset should be behind stateful firewall 3. Use secure tunnel communications channel		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
32	T02	Deliver directed malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
33	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A11	Smart medic app (Stryker Admin Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Deployed (V&V) secure system configuration model needs to be mentioned in the installation manual. 2. Establish internal and external information sources for threat intelligence and vulnerability data, monitoring them regularly and taking appropriate action for high-priority items 3. Use upgraded software, firmware 4. Never create/use credentials with personal details such as date of birth, spouse, or child's or pet's name 5. Stateful Firewall		
34	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
35	T02	Deliver directed malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
36	T02	Deliver directed malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A02	Tablet OS/network details & Tablet Application	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
37	T02	Deliver directed malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A11	Smart medic app (Stryker Admin Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	**LOW**	1. Identification of the sensitive data in storage and encryption of storage subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Use strong encryption algorithm		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
38	T03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
39	T03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A11	Smart medic app (Stryker Admin Web Application)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**MEDIUM**	1. Admin application can be accessed by login credentials & MFA. Hence, strong password policies & management are required 2. Data transfer between the admin application and the smart medic components needs to be encrypted & secured. 3. Any vulnerable network ports and connection points should be identified and hardened. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Stateful firewall		
40	T03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
41	T03	Gaining Access ([S]TRID[E])	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**MEDIUM**	1.During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Maintain Access Logs		
42	T03	Gaining Access ([S]TRID[E])	V01	Devices with default passwords needs to be checked for bruteforce attacks	A07	Interface/API Communication	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
43	T03	Gaining Access ([S]TRID[E])	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04	Authentication/Authorisation method of all device(s)/app	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**MEDIUM**	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3 Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		
44	T03	Gaining Access ([S]TRID[E])	V04	Checking authentication modes for possible hacks and bypasses	A04	Authentication/Authorisation method of all device(s)/app	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration		
45	T03	Gaining Access ([S]TRID[E])	V04	Checking authentication modes for possible hacks and bypasses	A11	Smart medic app (Stryker Admin Web Application)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration		
46	T03	Gaining Access ([S]TRID[E])	V04	Checking authentication modes for possible hacks and bypasses	A12	Smart medic app (Azure Portal Administrator)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks 2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks 4. Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
47	T03	Gaining Access ([S]TRID[E])	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
48	T04	Maintaining Access (TTP)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		
49	T04	Maintaining Access (TTP)	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04	Authentication/Authorisation method of all device(s)/app	1) Obtain knowledge about system internals 2) Attempt to find attack vectors 3) Possibilities for exploitation of publicly known Vulnerabilities.	NA	**LOW**	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		
50	T05	Clearing Track (TTP)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
51	T05	Clearing Track (TTP)	V23	Outdated - Software/Hardware	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
52	T05	Clearing Track (TTP)	V07	Lack of configuration controls for IT assets in the informaion system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malicious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
53	T05	Clearing Track (TTP)	V07	Lack of configuration controls for IT assets in the informaion system plan	A05	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
54	T05	Clearing Track (TTP)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
55	T05	Clearing Track (TTP)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
56	T05	Clearing Track (TTP)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A02	Tablet OS/network details & Tablet Application	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
57	T05	Clearing Track (TTP)	V10	The static connection digaram between devices and applications with provision for periodic updation as per changes	A05	Device Maintainence tool (Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
58	T05	Clearing Track (TTP)	V10	The static connection digaram between devices and applications with provision for periodic updation as per changes	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
59	T06	Elevation of privilege (STRID[E])	V15	Controlled Use of Administrative Privileges over the network	A04	Authentication/Authorisation method of all device(s)/app	1) Gaining access to the portal 2) Accessing confidential data, 3) Lead misuse of confidential data 4) Company defamation	NA	**LOW**	1. Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. 2. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. 3. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
60	T06	Elevation of privilege (STRID[E])	V15	Controlled Use of Administrative Privileges over the network	A12	Smart medic app (Azure Portal Administrator)	1) Gaining access to the portal 2) Accessing confidential data, 3) Lead misuse of confidential data 4) Company defamation	NA	**MEDIUM**	1. Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. 2. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. 3. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).		
61	T07	Denial of service (STRI(D)E)	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Bring down the service availability 2) Blocking the end user usage	NA	**MEDIUM**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
62	T08	Information disclosure (STR(I)DE)	V16	Unencrypted data at rest in all possible locations	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Identification of the sensitive data in storage and encryption of storage subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Use strong encrption algorithm		
63	T08	Information disclosure (STR(I)DE)	V17	Unencrypted data in transit in all flowchannels	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Use secure tunnel communication channel 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. For sensitive data proper encryption mechanism needs to be designed & implemented		
64	T08	Information disclosure (STR(I)DE)	V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Implement server-side encryption using Service-Managed keys/recomended practise by azure. 2. Proper way of network access control 3. Encryption for sensitive data in transit, for ex: when files are moved to cloud storage, etc.. 4. Transfer over encrypted tunnel 5. Use strong encryption algorithm		
65	T08	Information disclosure (STR(I)DE)	V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Statefull firewall 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Use secure tunnel communication channel		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
66	T08	Information disclosure (STR(I)DE)	V19	Weak Algorthim implementation with respect cipher key size	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Weak algorithms such as DES, RC4, etc.. should be avoided and usage of strong algorithms such as AES, RSA, etc.. are recomended 2. Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.		
67	T08	Information disclosure (STR(I)DE)	V19	Weak Algorthim implementation with respect cipher key size	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Weak algorithms such as DES, RC4, etc.. should be avoided and usage of strong algorithms such as AES, RSA, etc.. are recomended 2. Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.		
68	T08	Information disclosure (STR(I)DE)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
69	T08	Information disclosure (STR(I)DE)	V14	Unencrypted Network segment through out the information flow	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Anonymization/Pseudomyzation of patient details 2. Data encyrption 3. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 4. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.)		
70	T08	Information disclosure (STR(I)DE)	V05	Insecure communications in networks (hospital)	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc. .	NA	**LOW**	1. Secure communication with Secure Sockets Layer (SSL) or TLS protocols that provide message confidentiality 2. Secure sensitive data in the channel flow using strong encryption 3. Statefull firewall 4. Proper way of network access control		
71	T09	Data Access (STR[I]DE)	V12	Unprotected network port(s) on network devices and connection points	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		
72	T09	Data Access (STR[I]DE)	V12	Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	**LOW**	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		

ID #	Threat Event(s)		Vulnerabilities		Assets		Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
73	T09	Data Access (STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A09	Data at Rest	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	**LOW**	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Statefull firewall 3. Do not store sensitive data in plaintext. 4. Use strong encrption algorithm. 5. Apply salting over sensitive data.		
74	T09	Data Access (STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	**MEDIUM**	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Statefull firewall 3. Do not store sensitive data in plaintext. 4. Use strong encrption algorithm. 5. Apply salting over sensitive data.		
75	T09	Data Access (STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A10	Data in Transit	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	**LOW**	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Statefull firewall 3 Do not store sensitive data in plaintext. 4. Use strong encrption algorithm. 5. Apply salting over sensitive data.		
76	T09	Data Access (STR[I]DE)	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A09	Data at Rest	1) Allowing application or script to perform abnormal activites on the system. 2) Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. 3) Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	**LOW**	1. Strong password strength practices is recommended for admin web app. 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods		

Common Vulnerability Scoring System (CVSS v3.0)

Exploitability Metrics												
Attack Vector			**Attack Complexity**			**Privelege Required**				**User Interaction**		
Metric	**Value**	**Code**	**Metric**	**Value**	**Code**	**Metric**	**Value**		**Code**	**Metric**	**Value**	**Code**
Network	0.85	N	Low	0.77	L	None	0.85	0.85	N	None	0.85	N
Adjacent Network	0.62	A	High	0.44	H	Low	0.62	0.68	L	Required	0.62	R
Local	0.55	L				High	0.27	0.5	H			
Physical	0.2	P										

Likelihood of Attack Initiation	
Rating	Score
Very Low	0.04
Low	0.20
Moderate	0.50
High	0.80
Very High	1.00

Technical Impact Metrics		
Confidentiality, Integrity, Availability Impact		
Metric	**Value**	**Code**
None	0	N
Low	0.22	L
High	0.56	H

$ISC_{Base} = 1 - [(1-Impact_{Conf}) \times (1-Impact_{Integ}) \times (1-Impact_{Avail})]$

In Scope
Yes
No

Scope		
Unchanged	An exploited vulnerability can only affect resources managed by the same authority. In this case the vulnerable component and the impacted component are the same.	U
Changed	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case the vulnerable component and the impacted component are different.	C

ASSUMPTIONS:

Base metrics

For the purposes of the medical device only Base metrics are considered. The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.
The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
The document only considers the mandatory base metric since the device is typically utilized in tightly controlled user environments such as hospitals and this is already a consideration of this assessment document. The changing charecteristics of vulnerabilities will be assessed seperately through the software development lifecycle

Threat Sources

Adversarial Threat		
ID#	**Threat Source**	**In Scope (Y/N)**
TSA-1	Individual (Disgruntled/Ex-Employees, Outsider, Insider, Trusted Insider, Priveleged Insider)	Y
TSA-2	Organization (Competitor, Supplier, Partner, Customer, Researcher)	Y
TSA-3	Script Kiddies	Y
TSA-4	Political Activists (Hactivists, Anonymous, Wikileaks)	N
TSA-5	Organized Crime (Cyber Terrorists)	N
TSA-6	Nation States	N

Non-Adverserial Threat		
ID#	**Source**	**In Scope (Y/N)**
TSN-1	Accidental (Priveleged User/Administrator, inexperienced user, inexperienced installer, inexperienced maintainer, unintentional misuse)	Y
TSN-2	Researchers (Professional Security, Academic)	Y
TSN-3	Vulnerable systems/devices connected to device (e.g., via RS-232, USB, or other connections)	Y
TSN-4	Incompatible Software (OS, Networking, Applications)	Y
TSN-5	Environmental Impact (IT equipment, Temperature/Humidity Controls, RF Interference)	Y
TSN-6	Natural/Man-Made Disaster (Fire, Flood/Tsunami, Windstorm/Tornado, Earthquake, Bombing, Telecommunications/Power Failure)	N